Office of the Attorney General

Washington, D.C. 20530

September 11, 2014

MEMORANDUM TO THE UNITED STATES ATTORNEYS AND ASSISTANT ATTORNEY GENERALS FOR THE CRIMINAL AND NATIONAL SECURITY DIVISIONS

FROM: THE ATTORNEY GENERAL

SUBJECT: Intake and Charging Policy for Computer Crime Matters

Cyber-based crimes are one of the fastest growing threats our nation faces. Although laws addressing the misuse of computers have not kept pace uniformly with developments in technology and criminal schemes, the Computer Fraud and Abuse Act ("CFAA"), codified at Title 18, United States Code, Section 1030, remains an important law for prosecutors to address cyber-based crimes. As technology and criminal behavior continue to evolve, however, it also remains important that the CFAA be applied consistently by attorneys for the government and that the public better understand how the Department applies the law.

To accomplish these goals, I recently asked the Criminal Division to work with the National Security Division, the Executive Office of United States Attorneys, and the Attorney General's Advisory Committee to develop a policy to guide attorneys for the government in the appropriate considerations for prosecutors contemplating charges under the CFAA. The resulting policy is effective immediately.

A. *Policy.* In addition to the considerations set forth in USAM 9-27.230, which are incorporated herein by reference, an attorney for the Department of Justice should consider the following additional factors in determining whether prosecution of a violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, should be pursued because a substantial federal interest would be served by prosecution in a case in which the admissible evidence is expected to be sufficient to sustain a conviction. It is recognized that the significance of any cyber event for a District can vary depending on facts and circumstances specific to the District. Factors to be considered include:

1. The sensitivity of the affected computer system or the information transmitted by or stored on it and the likelihood and extent of harm associated with damage or unauthorized access to the computer system or related disclosure and use of information;

2. The degree to which damage or access to the computer system or the information transmitted by or stored on it raises concerns pertaining to national security, critical infrastructure, public health and safety, market integrity, international relations, or other considerations having a broad or significant impact on national or economic interests;
3. The extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm or a threat to national security;
4. The impact of the crime and prosecution on the victim or other third parties;
5. Whether the criminal conduct is based upon exceeding authorized access consistent with the policy set forth at page 4 below;
6. The deterrent value of an investigation or prosecution, including whether the need for deterrence is increased because the activity involves a new or expanding area of criminal activity, a recidivist defendant, use of a novel or sophisticated technique, or abuse of a position of trust or otherwise sensitive level of access, or because the conduct is particularly egregious or malicious;
7. The nature of the impact that the criminal conduct has on a particular District or community; and,
8. Whether any other jurisdiction is likely to prosecute the criminal conduct effectively, if the matter is declined for federal prosecution.

B. *Comment.* This policy lists factors that may be relevant in determining whether prosecution of violations of the CFAA should be pursued because a substantial federal interest would be served by prosecution in a case in which the person is believed to have committed an offense under the Act and the admissible evidence is expected to be sufficient to sustain a conviction. The list of relevant considerations and examples of criminal conduct illustrating those factors are not intended to be all-inclusive. Not all of the factors will be applicable to every case, and in any particular case one factor may deserve more weight than it might in another case. The principles set forth here, and internal office procedures adopted pursuant to this memorandum, are intended solely for the guidance of attorneys for the government. They are not intended to, do not, and may not be relied upon to create a right or benefit, substantive or procedural, enforceable at law by a party to litigation with the United States.

1. **Sensitivity of Affected Computer System or Information.** In determining whether to bring a charge for violation of 18 U.S.C. § 1030 in a case involving obtaining information from a protected computer, consideration should be given to the sensitivity and value of the information involved and the potential for harm associated with its disclosure or use. Examples of the types of information that should be given a high priority for federal prosecution when illegally accessed include sensitive personal information such as intimate photographs or correspondence, medical,

educational or financial records, Social Security numbers, biometric information, and other personal identification information, and passwords and access devices; trade secrets, valuable intellectual property, and other confidential business information; and classified or other sensitive government information. To be clear, federal prosecution may be warranted even where the offender did not actually obtain any such information; in other words, in certain aggravated circumstances, mere access to a computer system that stores these types of sensitive information may weigh in favor of prosecution. Further, federal prosecution may be warranted for conduct that involves accessing a computer system without authorization or in excess of authorization for the purpose of selling or trafficking in sensitive information or the public distribution of private information. Conversely, federal prosecution may not be warranted if the information obtained is otherwise publicly available or has little value.

2. **Potential for Broad or Significant Impact on National or Economic Interests.** Many types of offenses under the CFAA can have an impact far beyond the particular computer that is directly affected by the actions of the offender. Unauthorized access to a computer containing classified information, for example, can harm national security. Shutting down a computer that controls a portion of the electrical grid can harm business activities and put public safety at risk. Unauthorized access to stock market computers can undercut investors' faith in the fairness of the market. And the actions of terrorist organizations and foreign governments can cause significant harms to the safety and prosperity of Americans. Similarly, many types of malicious software can affect thousands of computers or more across the country and have the potential to invade the privacy and harm the financial security of those computers' users. Where criminal activity risks these broad harms or has a substantial effect in several parts of the country, federal prosecution may be warranted. In other circumstances, if the effect of a violation is geographically focused and limited, deference to state or local authorities may be warranted, where they have the legal tools and resources to act.

3. **Connection to Other Criminal Activity or Risk of Bodily Harm**. Offenses under the CFAA often occur in concert with, and in furtherance of, other criminal activity, including that which poses a threat to national security. Depending on the nature of the predicate criminal activity, such circumstances may weigh in favor of federal prosecution. Organized criminal enterprises, for example, access banking and financial computers to steal information in furtherance of fraud and extortion schemes. Individual hackers may gain access to the private information of others in order to stalk or harass, to encourage others to harass or endanger public officials and

other victims, or to profit from its sale. Disrupting a hospital computer can place patients' lives in danger.

4. **Impact of the Crime and Prosecution on Victim or Other Third-Parties.** An attorney for the government may consider whether investigation and prosecution might result in further negative impacts on victims or third-parties that cannot otherwise be avoided. Thus, prosecutors should take into account the impact of the crime on the victim, as detailed in USAM 9-27.230.

5. **Exceeding Authorized Access**. Several portions of the CFAA prohibit obtaining information by accessing a protected computer either (1) without authorization, or (2) in a manner that "exceeds authorized access." Some exceeds-authorized-access violations may occur where the actor had authorization to access the computer for one purpose but accessed the computer for a prohibited purpose. For example, in several circuits, violation of the statute under the exceeds-authorized-access theory might occur where an employee accesses sensitive corporate information in violation of the company's access policy, or where a law enforcement officer accesses the National Crime Information Center ("NCIC") computers to obtain information in order to stalk a former romantic partner, which would violate NCIC's access restrictions.

   When prosecuting an exceeds-authorized-access violation, the attorney for the government must be prepared to prove that the defendant knowingly violated restrictions on his authority to obtain or alter information stored on a computer, and not merely that the defendant subsequently misused information or services that he was authorized to obtain from the computer at the time he obtained it. As part of proving that the defendant acted knowingly or intentionally, the attorney for the government must be prepared to prove that the defendant was aware of such access restrictions.

   The extent of the federal interest in exceeds-authorized-access prosecutions under section 1030(a)(2) varies based upon both the nature of the conduct and the nature of the information obtained during the offense. As with situations presenting an increased need for deterrence, one factor that supports prosecutions under the exceeds-authorized-access provision is the abuse of a position of trust. Examples would include situations in which a system administrator invaded the privacy of email accounts in violation of company policy and for personal gain, or in which a government official accessed information stored on government computers in contravention of clear rules prohibiting such access. Likewise, if the criminal conduct threatened national or economic interests, was in furtherance of a larger criminal endeavor, or posed a risk of bodily harm or threat to national security, those

factors would weigh in favor of prosecution. On the other hand, if the defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website, federal prosecution may not be warranted.

6. **Increased Need for Deterrence.** As technology advances, criminals discover novel ways to exploit it. For example, as mobile devices become increasingly powerful and flexible, they have also increasingly become a target for computer criminals. An individual may also abuse a trusted position to commit a computer crime, or may exhibit particularly malicious motivation or egregious behavior. These considerations may, in combination with other factors, weigh in favor of federal prosecution.

7. **Extent of Harm to One District or Community.** In deciding whether to bring a CFAA prosecution in a particular District, the attorney for the government should consider how much harm the criminal activity caused within the relevant District or community. Where an offense causes particularly significant harm to a single District or community, federal prosecution may be warranted.

8. **Possibility of Effective Prosecution in Another Jurisdiction.** In determining whether prosecution should be pursued even though the person is subject to effective prosecution in another jurisdiction, the attorney for the government should weigh the considerations discussed in USAM 9-27.240.

C. *Consultation.*

1. **Introduction**

Cases under the CFAA are often complex, and analysis of whether a particular investigation or prosecution is warranted often requires a nuanced understanding of technology, the sensitivity of information involved, tools for lawful evidence gathering, national and international coordination issues, and victim concerns, among other factors. USAM 9-50.000 sets forth general requirements for cyber prosecutions, including coordination with and notification of the Computer Crime and Intellectual Property Section ("CCIPS") of the Criminal Division in certain cases. These provisions are still in effect.

2. **Investigative Consultation**

In addition, at important stages of an investigation, because it is the best practice, the attorney for the government should consult with a Computer Hacking and Intellectual

Property Coordinator ("CHIP") within the District in which the case would be brought. Because electronic evidence is often subject to deletion after very short retention periods, the need to preserve or obtain evidence critical to the investigation may require taking preliminary investigative steps before undertaking the consultation above. In such cases, the consultations, as required, should take place as soon as possible.

3. **Charging Consultation**

With respect to charging decisions, the attorney for the government shall consult with CCIPS, which often has knowledge of similar cases in other Districts or how the case may fit into national priorities. Attorneys for the government are encouraged to have a District CHIP participate in this consultation. The consultation should be substantive in nature. It is meant to both assist the prosecutor and promote consistency in the Department in a quickly evolving area of practice. The depth of the consultation and degree of information required to accomplish these goals will vary according to the facts, complexity, and sensitivity of a particular investigation or matter. These types of consultations are already a hallmark of the CHIP program, and the strong working relationships are a key reason for the program's collaborative successes.

4. **Consultation for Cases Involving National Security Issues**

For CFAA cases involving international terrorism or domestic terrorism, or affecting, involving, or relating to the national security, USAM §§ 9-2.136, 9-2.137, 9-90.020, and/or 9-90.800 set forth additional National Security Division notification, consultation, and approval requirements. In such cases, the attorney for the government can, if he or she chooses, satisfy the initial CCIPS and NSD notification requirements with one contact. NSD or CCIPS will then be responsible for facilitating any additional required notifications, consultations, or approvals, including, to the extent requested by the attorney for the government, with the other component. If there is any question about whether a matter involves international terrorism, domestic terrorism or otherwise affects, involves, or relates to the national security, the attorney for the government should consult with the National Security Cyber Specialist (NSCS) within his or her district for further guidance.